Secure and Trustworthy Cyberphysical Microfluidic Systems

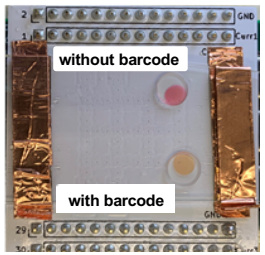
Challenges:

- Vulnerabilities to biochemical, malicious cyber-physica,l and intellectual-property (IP) threats
- Biochemical threats: Sample tampering
- Malicious threats: Structure-based (SB) and Material-based (MB) attacks
- IP-theft threats: Counterfeiting and overbuilding attacks

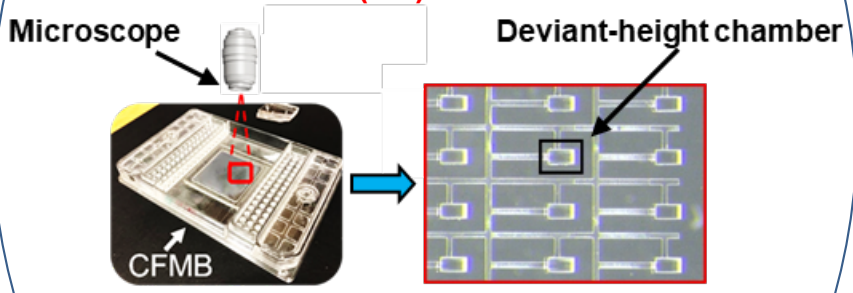
Advances and Solutions:

- Molecular barcoding: DNA samples uniquely barcoded using loop-mediated isothermal amplification (LAMP) reactions
- Demonstrated SB attack using a commercial biochip as a reference
- Machine learning-based anomaly detection algorithm to detect microstructural faults in CFMBs
- Novel device-level watermarking scheme against IP-theft attacks

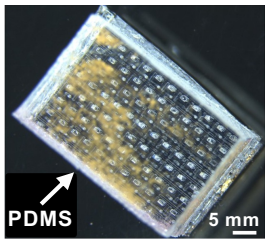
Molecular Barcoding



Structure-Based (SB) Attack-Defense Model



Material-Based (MB) Attack-Defense Model



NSF SaTC Award 2049335
Duke University and New York University
Contact: *rkarri@nyu.edu*, and *krish@duke.edu*

Scientific Impact:

- Ensure security and trustworthiness of biochips used for medical diagnostics and research
- Highlight various attacks surfaces and provide countermeasures to circumvent the attack
- Add knowledge and understanding toward stealthy attacks to enable rational countermeasures

Broader Impact and Broader Participation:

- Safeguard biochips in the era of global pandemics and personalized medicine
- Enable authenticity of manufactured biochips
- Reach and educate clinicians and researchers worldwide
- Molecular diagnostics market projected to be $31.8 billion by 2026, up from $17.8 billion in 2021
- Female and LatinX PhD students recruited